Indiana Water Treatment Plants and Utilities Required to Reinforce Cybersecurity Defenses

May 29, 2025

Categories:

Publications
Technology Blog

Authors:

Gene F. Price
Matthew R. Schantz
Robert W. Dibert

It is well known that malicious actors have been targeting the U.S.'s critical infrastructure through cyberattacks. These attackers usually target the operating technology of our water infrastructure by exploiting the internet access of a given plant.

This alarming trend was all too evident when a water treatment plant in Tipton, Indiana, fell victim in April 2024 to hackers who breached its cybersecurity defenses, disrupting its operations. Fortunately, the disruption was minimal, and the plant remained operational, but the incident raised fears of more attacks when Russian hackers claimed responsibility for the Indiana attack, claimed to have successfully attacked a Texas water treatment plant, and stated there would be more to come.

To preempt these threats, Indiana's legislature passed Senate Bill 459, which goes into effect on July 1, 2025. SB 459 requires Indiana water treatment plants to strengthen their cybersecurity defenses to make it harder for any hacker to get into Indiana's water supplies.

Accordingly, if you operate a community water system in Indiana that serves a population of at least 500, or a publicly or semipublicly owned water treatment facility that uses a central computerized system to control operations or another similarly vulnerable system as identified by the Department of Environmental Management, you must do the following:

- Conduct a cybersecurity vulnerability assessment at least once a year.
- Provide the Office of Technology with the name and contact data of the person who will serve as the primary reporter of any cybersecurity incident by September 1 of each year.
- Certify to the Department of Environmental Management via a secured portal that you have completed the assessment, mitigated or documented plans to mitigate identified

vulnerabilities, and updated emergency response plans accordingly—no later than December 31 of each even-numbered year, beginning in 2026.

- When an actual or suspected cybersecurity breach occurs, report the incident in prescribed format to the Office of Technology within 24 hours if operations were impacted or within two business days if they were not.

Indiana clients in the water treatment sector should note these requirements and ensure they are complying with them in advance of SB 459's effective date (July 1, 2025). For additional information or assistance complying with the new requirements, contact the authors of this article or any member of Frost Brown Todd's Data Security and Privacy team.

**Prabha Rajasekaran, a second-year law student at the University of Louisville Brandeis School of Law, contributed to this article while working as a summer associate at Frost Brown Todd.*

FBT Gibbons